A HYBRID GROUP BASED RE-KEY MANAGEMENT SCHEME FOR SECURE COMMUNICATION IN WIRELESS SENSOR

S. SUMA CHRISTAL MARY† and M. PALLIKONDA RAJASEKARAN‡

† Computer Science and Engineering, Kalasalingam University, Krishnankovil, Tamil Nadu, India.
‡ Electronics and Communication Engineering, Kalasalingam University, Krishnankovil, Tamil Nadu, India.
Email: sumachristy2012@gmail.com

Abstract — Secured Communication is primarily important in Wireless Sensor Networks (WSNs), since the communication signals are explicitly available as they broadcast through the air. These networks are more vulnerable to attacks extending from passive eavesdropping to active snooping. In this paper, a hybrid Group based Re-Key Management Scheme (HG-RMS) is proposed. The objective of this paper is to provide a secure group communication in WSNs. The Group Controller is elected for each group to manage the group members. The proposed HG-RMS incorporates the Modified Hybrid Energy Efficient Distributed (M-HEED) protocol to elect the group controller. Rivest Shamir Adleman (RSA) is used by the Key Management Center (KMC) to generate the keys and distribute to the group controllers. The key exchange mechanism is explored for secure communication between the users. Node compromise attacks are detected and prevented based on the periodic broadcast messages. The re-keying process is initiated whenever a node joins/leaves the group. The experimental results show that the proposed scheme performs better than the existing Cluster based Group Key Management (CB-GKM) in terms of energy, privacy level, memory, and time consumption.

Keywords — Diffie Hellman, Modified Hybrid Energy Efficient Distributed (M-HEED), Key Management Center (KMC), Node Compromise Attack, and Rivest Shamir Adleman (RSA).

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have recently developed as a platform for numerous important surveillance and control applications (Rahman, 2010). Generally, sensor nodes stay fewer mobility, more limited in capabilities and more densely deployed than the Mobile Adhoc Networks (MANETs). The sensor nodes gather the information and route the information to the base station. All of the nodes are not essentially communicating at any particular time and nodes can only transfer with a few nearby nodes. The network has a routing protocol to regulate and control the routing of data messages between nodes. Moreover, Grouping is an essential practice to localize computation and decrease the communication overhead in WSNs (Wang et al., 2010). The most standard method of grouping is clustering. The main operation in the sensor node grouping is to choose the set of group controllers or group heads among the sensor nodes (Klaoudatou et al., 2011). The group controller nodes are responsible for organizing among the nodes and communications between the nodes. Many routing protocols and key management protocols have been proposed already. Usually, the cluster has a cluster head node and the group contains the group controller node. The main difference between clustering and grouping are: Clustering is a universal concept, whereas grouping is typically focused on a small area. A group can be a part of the cluster or may be the union of several clusters.

Security is the most important research domain in the field of wireless sensor networks. The secure group communication is based on the trusted transmission of the group key between valid nodes in a group. It includes the communication between the nodes that are eligible to send and receive the messages to the group. The major problem of secure group communication is key management. An asymmetric group key known only to group nodes and the key server is used for encrypting the data traffic among the group users. The group key access is controlled by the group key management system. It sends the group key to certified new users and also performs the rekeying process whenever the node joins/leaves the network. Precisely, a group key management model can implement two kinds of access control (Wen et al., 2012): backward access and forward access control (Alzaid et al., 2010). If the group alters the group key after the new node joins, the new node may not be able to decrypt the past communications; this is termed as a backward access control. If the group rekey after a current node leaves, then the departed node may not able to access the future communications; this is referred as forward access control.

Yang et al. (2013) proposed an Identity Based Key Agreement Scheme (IBKAS). This scheme was based on identity based encryption and Elliptic Curve Diffie Hellman (ECDH). This scheme prevents the man in the middle attacks and node capture attacks by encrypting the key agreement parameters (Yang et al., 2013). Lin et al. (2010) designed a key management scheme for sensor networks based on bilinear pairings and Diffie Hellman group. This scheme ensures that any node pair can steadily assign one session key (Lin et al., 2010). Yuan et al. (2010) proposed a cluster based group key management approach for WSN. A group key was created by the association of cluster head and nodes within the particular cluster. Cluster heads were responsible to reconstruct and transfer the group key (Yuan et al., 2010). The advantage of secure group communication is that outside nodes are not able to get the messages. The group controller node is used to gather the similar data in order to reduce the communication overhead. Nowa-